DEPARTMENT OF THE NAVY
NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER

NAVSO P-5239-29
JULY 1994

CONTROLS OVER COPYRIGHTED COMPUTER SOFTWARE

GUIDEBOOK

MODULE 29

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commander
Naval Information Systems Management Center
Code 05
1225 Jefferson Davis Hwy.
CG2, Suite 1500
Arlington, VA 22202-4311
Commercial (703) 602-6799
DSN 332-6799

Stocked: Additional copies of NAVSO P-5239-29 can be obtained from the Naval Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia, PA 18120-5099, through normal supply channels in accordance with NPFC PUB 2002D, NAVSUP P-437 or NAVSUP P-485, using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8360.

Local reproduction is authorized.

FOREWORD

This publication, Navy Staff Office Publication (NAVSO Pub) 5239-29, "Controls Over Copyrighted Computer Software" is issued by the Naval Information Systems Management Center (NISMC).

This publication provides Department of the Navy (DON) activities with guidance and recommended procedures for implementing "internal management controls" to ensure compliance with copyrighted computer software agreements.

The responsibility for "internal management controls" is under the authority of the Commanding Officer (CO) or the Designated Approving Authority (DAA). A Responsible Officer will be identified by the CO or DAA to implement internal management control procedures to **ensure** that copyrighted computer software agreements are being properly followed within the command. The placement of this authority decision rests **within each activity**.

This publication's goal is to assist DON activities as a "get well process" and not as a means for "tagging" copyright violators. The general purpose of this publication is to assist DON activities in developing and implementing their **own policies and procedures** for controlling and using computer software programs having licensing agreements and copyright protection within the DON.

Instructions herein are issued for the information and compliance of all persons in the DON and are effective upon receipt.

J. G. HEKMAN
Rear Admiral, SC, USN
Commander

TABLE OF CONTENTS

CHAPTER 1

GENERAL INFORMATION

1.1. **Purpose**. This document provides guidance and procedures for implementing controls over copyrighted computer software throughout the Department of the Navy (DON). Numerous DoD instructions such as DoD Instruction 7920.5, and SECNAV Instruc-tions 5239.2 and 5870.5 have established policy to enforce the software licensing provisions of the contractual vehicle used to obtain commercial software and ensure compliance with the terms and conditions for commercial software use, including **copyright** and license agreements.

1.2. **Introduction**. During 1993, DoDIG Audit Report No. 93-056 identified material weaknesses in the internal controls designed to monitor the installation and accountability of copyrighted computer software programs. This audit showed that 51 percent of the 1,022 computers tested within the DoD had copyrighted software programs installed without documentation to prove that the software had been legally acquired. It should, however, be understood that this did not prove "illegal" use, but rather poor record keeping. Unauthorized use of copyrighted computer software contravenes federal laws and denies software vendors their rightful revenues.

a. As stated in DoDIG Audit Report No. 93-056, copyrighted computer software programs are used on approximately 400,000 microcomputers throughout DoD. It is estimated that there are more than 175,000 microcomputers using copyrighted computer software within the DON. DON does not maintain "centralized" records on the number of software programs on hand, but a good estimate suggests that millions of software programs are resident in DON microcomputers.

b. Federal copyright law grants copyright owners exclusive rights to duplicate or distribute the programs. Although software vendors attempt to control unauthorized use of their products through licensing agreements that invoke the protection available under copyright statutes, compliance with licensing agreements relies on the integrity of the software user.

c. The specific license agreement for each software product is explained in documentation accompanying the system disks that enable the user to install and operate software

programs on a computer. Although the wording may differ slightly, license agreements specify that each software program purchased is to be used on a specified number of computers at one time. Also, an activity may purchase a "site license" or a license to use a software program on a local area network (LAN). Such licenses permit an activity to use the covered software program by a specified number of users at any given time as stated on the agreement. Rather than incorporating built-in controls to disable software from being copied, most vendors attempt to control unauthorized use of their products through licensing agreements that invoke the protection available under copyright statutes. Thus, as previously stated, compliance with licensing agreements relies on the integrity of the software user.

d. There are many questions and considerations that need to be addressed by each activity before they establish and implement their own internal management controls for copyrighted computer software usage. This guidebook's purpose is to alert the DON activities of the problem, suggest processes and procedures to correct the problem and recommend that corrective actions be initiated immediately by each activity.

1.3. **Copyright Laws**. Title 17, United States Code, Section 106 gives owners of copyrights the exclusive rights to reproduce, distribute, or make derivative works of their material. Section 504 of the statute states that a copyright infringer is liable for actual damages to a copyright owner or statutory damages up to $100,000.

a. On 12 December 1980, Public Law 96-517 was enacted to give software specific coverage under the Copyright Revision Act of 1976 (effective 1 January 1978). The Copyright Revision Act of 1976 gives certain rights (17 U.S.C. § 117) to users which had been prohibited under the Copyright Revision Act of 1976 (17 U.S.C. § 106). Title 28 United States Code, Section 1498 enables owners of commercial software copyrights to take action against the federal government for copyright infringement.

b. Title 17, United States Code, Section 117 provides that it is not an infringement of copyright for a licensed user to make a copy of copyrighted computer software or programs if that copy is created "as an essential step in the utilization of the computer program" or "for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful."

c. Public Law 102-561 of 28 October 1992 describes in detail criminal penalties for copyright infringements. There are many aspects to the protection of copyrighted materials, including software, that are not presented here. The reader should not assume that these are the only laws pertaining to the subject. However, they are the essential ones specifically regarding software.

d. Appendix A addresses a series of the "most-asked" questions pertaining to copyrighted computer software and equipment.

1.4. **Policy**. As identified in DoDINST 7920.5, it is DoD policy to:

a. Enforce the software licensing provisions of the contractual vehicle used to obtain commercial software.

b. Inventory and report End User Computing (EUC) systems, which include software, to the Defense Automation Resources Information Center (DARIC), in accordance with DoD 7950.1-M.

c. Establish effective internal management systems controls for EUC systems.

1.5. **Responsibilities**

a. Commanding Officers or Designated Approving Authorities shall:

(1) Establish uniform policies and procedures to ensure that all DON activity personnel are made aware of their responsibility associated with copyrighted computer software programs. Appendix E has a sample memorandum of understanding that may be practical for organizations to use.

(2) Develop plans for achieving compliance with Copyright Laws.

(3) Ensure that annual reviews are conducted for evaluation of how the processes and procedures are meeting their goals. Take action to correct any deficiencies discovered.

b. The Responsible Officer shall:

(1) Prepare, issue, and update the Command's procedures and guidance to ensure that all aspects of copyrighted computer software laws are being complied with appropriately.

(2) Monitor the organization's implementation of these procedures.

1.6. **Procedures**. The following are **suggested** actions/steps for developing an organization's internal control process. Each activity shall establish its own internal process/controls that will support their mission and address the following criteria:

a. Establish and distribute to all employees, the activity's policy and internal process for addressing the use of copyrighted computer software.

b. Consider establishing supervisory/staff training to explain the roles and responsibilities associated with the organization's internal process for controlling copyrighted computer software usage.

c. Survey the organization's computers and identify all copyrighted computer software resident on each computer. (This type of survey may be able to serve a multitude of requirements, beyond just copyrighted software accountability.)

d. Forward this information to the Responsible Officer for establishing and maintaining a database of inventory.

e. Validate software purchase accountability by verifying contract documentation, purchase agreements, etc.

f. Determine the software that is necessary for job performance.

g. Consider establishing a local software users group/ software standards team.

h. Consider purchasing census-type software management tool(s) that will electronically inventory PC hard drives and network servers to identify the resident software.

i. Perform an audit, at least annually, to validate that the internal controls are satisfactorily meeting the Organ-ization's established goals and objectives.

The Responsible Officer, working closely with the Commanding Officer/DAA and the Organization's Legal Counsel, will determine further appropriate actions.

A sample survey, for inventory purposes, is outlined in Appendix C. A "boiler-plate" or sample set of procedures is outlined in Appendix F.

APPENDIX A

QUESTIONS MOST ASKED ABOUT COPYRIGHTED COMPUTER SOFTWARE

PLEASE REFER SPECIFIC QUESTIONS TO YOUR ORGANIZATION'S LEGAL COUNSEL. THE RESPONSES TO THE FOLLOWING QUESTIONS ARE NOT TO BE ACCEPTED AS LEGAL COUNSEL BUT RATHER AS GENERAL GUIDANCE.

Q1. WHAT ARE THE RULES ON USING GOVERNMENT COMPUTER EQUIPMENT?

Answer. The ready accessibility of office automation equipment has led to the misuse of word processors, computers, and software. Vendor supplied software **may not** be reproduced for distribution other than to authorized government agencies, according to the terms and conditions of the contract. If you violate copyright laws and other conditions of a software licensing agreement, you are acting on your own accord, and disciplinary action may be taken against you.

Q2. HOW MANY "BACKUP" COPIES OF THE APPLICATION SOFTWARE CAN BE MADE BY A USER?

Answer. There is no specific number that can be given because each organization has developed their own evaluation of "comfort" when they deal with "backups." Therefore, each organization may make as many copies as they deem necessary but these backups are to be used only when the originals fail. The intent of a "backup" is primarily to be treated as an alternative or substitute **kept in reserve for an emergency**.

Usually, it is suggested that the master disk be "write protected" when it is taken from the package, copied, and then the copy used to load the software. Sometimes, a second copy will be made to be stored at some off-site location as part of a contingency plan. Backup procedures covering other mechanisms such as tape, removable hard drives, optical storage, etc. need to be documented.

Q3. CAN I TAKE GOVERNMENT-OWNED APPLICATION SOFTWARE HOME TO USE ON MY PC WHEN WORKING ON A GOVERNMENT PROJECT?

Answer. To the uninitiated, it would appear logical and sensible to do this when the effort is in the best interest of the government and the employee agrees to delete the software

from his/her PC at the end of the effort. However, be warned, that most legal points of contact in DON activities believe the answer to this question is **"NO."** It is important for this question to be answered on a case-by-case basis by your rganization's legal counsel.

Q4. WHERE DOES THE LICENSING AGREEMENT DOCUMENTATION EXIST IN DON ACTIVITIES?

Answer. This varies from activity to activity. The Responsible Officer should confer with the administrative personnel and the purchasing/procurement personnel to determine where records are kept for their activity.

Q5. WHAT VALUES, ECONOMICALLY/TECHNICALLY, DOES A SITE LICENSING AGREEMENT GIVE AN ORGANIZATION?

Answer. Depending on the terms of the site license, it may or may not be more economical. Often, the purchase of a site license for a software package can result in lower costs per unit of software. If a multi-user license is purchased for use on a network server, the license can often serve more individuals than the license was intended for. For example, if the multi-user license is for 10 simultaneous users, but there are 24 people in the activity, this means that only 10 people at a time can access the software. Frequently, between travel, sick and annual leave, amount and type of usage, etc., there are very seldom going to be more than 10 people who want to access the software simultaneously, so there won't be a problem. If the occasion does occur where an 11th user tries to access the software, such a package will usually inform the employee that access is denied and to try again at a later time.

Another example for potential savings is the cost of documentation. For example, in the situation where many VAX work stations are installed at a site, there may be a need for only one or two sets of documentation. Since the documentation is sold separately from the software, this could result in considerable savings for the activity.

For activities that centrally control the purchase and installation of software onto their systems, a site license may be easier to manage from an inventory and logistical perspective.

Q6. WHAT DO WE DO IF WE CAN'T PROVE OWNERSHIP OF THE COPYRIGHTED SOFTWARE THAT WE ARE USING?

Answer. First, discuss this problem with your Responsible Officer and, if need be, your organization's Legal Counsel. Hopefully, the organization will have a policy to address this question. However, in the meantime, if **software** resides on a computer which you aren't using to perform your responsibilities, and documentation is not available to identify ownership, it is recommended that you remove the software and notify the Responsible Officer immediately.

Q7. MAY I LOAD MY PERSONALLY-OWNED SOFTWARE ONTO A GOVERNMENT COMPUTER IF NEEDED TO PERFORM MY JOB?

Answer. Generally, the answer is **"NO."** However, it is recognized that there may be mitigating circumstances which would allow such action. It is recommended that each activity which would consider allowing such action have a procedure which allows one to do this only after receiving authorization from the Commanding Officer or the DAA. In the agreement, the owner of the software must state that he/she agrees to be liable for compliance with the licensing agreement. The **Responsible Officer** should file the "originals" of all such agreements and have them readily accessible in the case of an audit.

APPENDIX B

DEFINITIONS

APPLICATION SOFTWARE : **Programs that perform useful functions in the processing or manipulation of data; includes database managers, word processors, spreadsheets, telecommunications, desktop publishers, and other programs that manipulate data.**

AUTOMATED INFORMATION SYSTEMS (AIS) : **Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition; storage; manipulation; management; movement; control; display; switching; interchange; transmission or reception of data and includes computer software, firmware, and hardware.**

DESIGNATED APPROVING AUTHORITY (DAA) : **Official with the authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk.**

FREEWARE : **Copyrighted software that has been made available to the public without cost, is distributed from an authorized source, and which may have restrictions regarding use, further distribution or resale.**

LICENSE : **An agreement by a contractor to permit the use of copyrighted software under certain terms and conditions.**

LOCAL AREA NETWORK : **An interconnected collection of components that are physically located within a small geographic area, such as a building or campus.**

NETWORK : **A system that is implemented with a collection of interconnected components.**

NETWORK SERVERS : **A network device that normally houses the Network Operating System and common-use files.**

PERSONAL COMPUTER (PC) : **A microprocessor-based computer which is primarily intended to be used by one person at a time. It is usually characterized by relatively low cost and small physical size (usually small enough to fit on a desk or table).**

PUBLIC DOMAIN SOFTWARE : **Software not copyrighted that can be freely distributed without obtaining permission from the author or paying the author a fee.**

RESPONSIBLE OFFICER (RO) : **An individual appointed by proper authority to exercise custody, care, and safekeeping of property entrusted to that individual's possession or under their supervision; may include financial liability for losses occurring because of failure to exercise this obligation.**

SHAREWARE : **Copyrighted computer software distributed on a trial basis with a license to use for a "limited" period of time. Shareware is distributed by making it available on a computer bulletin board or by encouraging holders of the software to allow others to copy it. Use of shareware beyond the limited period may carry an obligation to pay the copyright owner. Payment usually takes the form of a registration fee for which the user may get a manual, support and updates. Further distributions by shareware holders are made under the same conditions of trial and implied obligation to pay.**

SITE LICENSE : **The use of the terms Site License, Corporate License, and Enterprise License all have meanings associated to large quantity purchases. Therefore, the associated definitions for these terms are more accurately set by the contracting officer and the company licensing the software. For the purpose of this document all of these items will be referred to as "Site License."**

APPENDIX C

COMPUTER SOFTWARE SURVEY

Name: _____

Code: _____

Supervisor: _____

Building No: _____
Room No: _____

Computer Model Type: _____
Computer Serial No: _____
Computer Bar Code ID: _____

(Description, Model No, Serial No, Bar Code)

Peripherals: _____ _____ _____ _____
_____ _____ _____ _____
_____ _____ _____ _____
_____ _____ _____ _____

Connected to a LAN(s) Yes _____ No _____

If "yes," specify the name of the LANs the computers connected to or has access to through data lines:

_____
_____
_____
_____
_____

List all software resident on this Computer:

(Vendor)	(Software Title)	(Version)	(License Documentation) State Lic.#	Serial #

APPENDIX D

MANAGEMENT CONSIDERATIONS FOR EFFECTIVELY MANAGING COPYRIGHTED COMPUTER SOFTWARE

The following is a list of questions that each activity's management should consider before they establish, publish and enforce its policies and procedures for controlling copyrighted computer software:

A. Which office shall be designated as the Activity's Responsible Officer for ensuring that the policy and procedures for internally managing copyrighted computer software are being met? (Security, IRM-Admin, Logistics, etc.)

B. Should it be a civilian or military billet assignment? (The civilian billet may allow more stability due to rotation of officer assignments and give the activity a chance to establish and document "corporate knowledge.")

C. Should a training program be established for the Responsible Officer and staff?

D. Should each employee attend an annual training awareness program?

E. Should the annual training/awareness be tied in with the annual ethics or security training awareness program?

F. Should each employee be required to sign a "Memorandum of Understanding" as described in Appendix F?

G. How often should an activity perform an inspection to verify and validate that the software resident on each computer has been properly obtained?

H. Should the inspection address "sample" population or all computers at the command?

APPENDIX E

(SAMPLE)

MEMORANDUM OF UNDERSTANDING FOR THE USERS OF COMMERCIAL SOFTWARE

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE COMMANDER OF _____
AND
PERSONNEL OF THIS COMMAND USING COMMERCIAL SOFTWARE

SUBJECT: Copyrighted Computer Software Policy

1. I understand that software will only be used in accordance with the software licensing agreement.

2. I understand that if I knowingly make, acquire, or use unauthorized copies of computer software, I may be subject to discipline according to the circumstances.

3. I understand that pursuant to federal statute, illegal reproduction of commercial software use is subject to civil damages up to $100,000 (for willful infringement) and criminal penalties to include fines and imprisonment for multiple reproductions for commercial purposes or private financial gain in accordance with Title 17, United States Copyright Code, Sections 504 and 506.

4. I have read and understand the software protection policies of this activity and will abide by them.

_____
SIGNATURE/DATE

_____
NAME/GRADE

_____
ORGANIZATION/TELEPHONE NO.

APPENDIX F

(SAMPLE)
PROCEDURES
USED FOR INTERNAL CONTROLS
TO MANAGE COPYRIGHTED COMPUTER SOFTWARE

A. A **Responsible Officer/Office** needs to be assigned the responsibility to develop, establish and implement a process and procedure for controlling the use of copyrighted computer software.

B. The organization distributes **policy** to all personnel explaining why these internal controls are required and how the organization plans to implement its **process**. This **policy** will identify when this **process** goes into effect and how each office is to implement it.

C. The **survey**, as described in Appendix C or a survey that is developed by the organization needs to be distributed through each office's management personnel with an established date for completion and return to the **Responsible Officer**.

D. The survey information must be maintained as an **inventory** database for the organization. This database will be updated periodically as stated in each organization's **policy** statement.

E. The **Responsible Officer** with the assistance of each office will then validate the survey information with proof of purchase, licensing agreements, and any other invoice information which will show proof of ownership for accountability and **validation**.

F. When the above step is completed, the Responsible Officer will report the findings to the **Commanding Officer** of the activity.

G. Corrective actions, if required, should then be directed by the Commanding Officer.

H. This process must be institutionalized as an annual process. It is not a "single-time" action.